PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-185445
(43)Date of publication of application : 16.07.1996

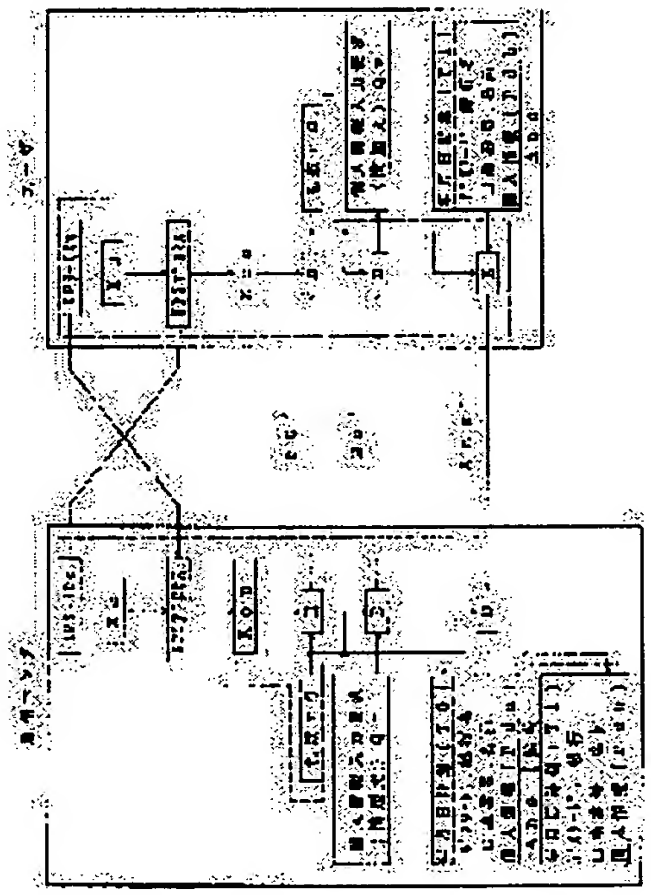
(51)Int.CI. G06F 17/60
H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : 06-337673
(22)Date of filing : 28.12.1994

(71)Applicant : ADVANCE CO LTD
(72)Inventor : WATANABE SHINICHIRO

(54) AUTHENTICATION SYSTEM AND TRANSACTION SYSTEM USING THE AUTHENTICATION SYSTEM

(57)Abstract:
PURPOSE: To make possible easy and safe authentication and exclusive one merchandise transaction based on it by authenticating a right user and forming a network to be used by the user without anxiety.
CONSTITUTION: An object to be authenticated is provided with an area which is secret or can not be altered, and arbitrary information sent from a source authentication object or a rule previously set with the source authentication object is stored in this area temporarily or for a prescribed term. Then, return data composed of the arbitrary information, data based on this arbitrary information or data based on the rule are sent to the source authentication object.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平8－185445

(43)公開日　平成８年(1996)７月16日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　17/60					
Ｈ０４Ｌ　9/00					
9/10					
			Ｇ０６Ｆ　15/21	３４０　Ｂ	
			Ｈ０４Ｌ　9/00	Ｚ	

審査請求　未請求　請求項の数５　ＦＤ　（全９頁）　最終頁に続く

(21)出願番号　特願平6－337673

(22)出願日　平成６年(1994)12月28日

(71)出願人　000126757
株式会社アドバンス
東京都中央区日本橋小舟町５番７号

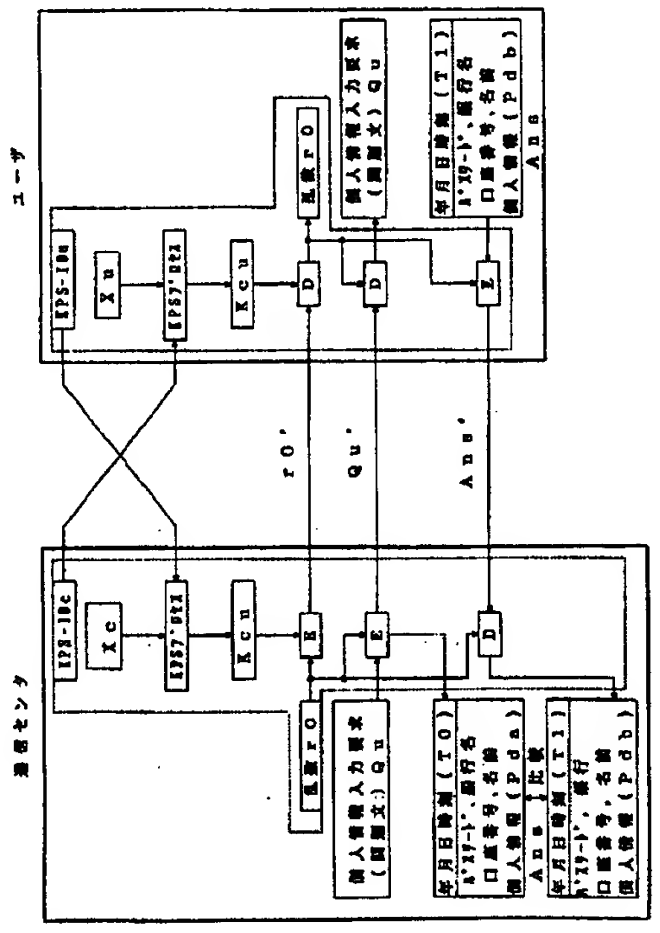
(72)発明者　渡辺　晋一郎
東京都江戸川区小松川１－２－３　コーシャタワー小松川902

(54)【発明の名称】　認証方式及び同方式による取引システム

(57)【要約】

【目的】正当な利用者の認証ができ、利用者が安心して使用できるネットワークが形成され、簡便で安全な認証及びそれに基づく唯一の商品取引を可能にする。

【構成】被認証体は秘密又は改暫不可能な領域を有し、原認証体から送付された任意情報乃至予め原認証体間で設定された取り決めを該領域に一時的又は所定の期間保持し、該任意情報乃至該任意情報に基づいたデータ乃至該取り決めに基づいたデータよりなる戻りデータを原認証体に送付する。



1

【特許請求の範囲】

【請求項１】被認証体は秘密又は改ざん不可能な領域を有し、原認証体から送付された任意情報乃至予め原認証体間で設定された取り決めを該領域に一時的又は所定の期間保持し、該任意情報乃至該任意情報に基づいたデータ乃至該取り決めに基づいたデータよりなる戻りデータを原認証体に送付することを特徴とする認証方式及び同方式による取引システム。

【請求項２】原認証体はリクエスト及び任意情報を被認証体に送信し、被認証体は該戻りデータとリクエストに基づくデータを原認証体に送付し、原認証体は任意情報と戻りデータとを比較する請求項１に記載の認証方式及び同方式による取引システム。

【請求項３】原認証体はリクエストを被認証体に送信し、被認証体は、該取り決めに基づく戻りデータとリクエストに基づくデータを原認証体に送付し、原認証体は該取り決めに基づくデータと該戻りデータとを比較する請求項１に記載の認証方式及び同方式による取引システム。

【請求項４】原認証体は、商品乃至サービスを提供する側であり、被認証体は、提供を受ける側であって、すくなくとも商品乃至サービスの提供が行われた時、提供を受けた側は、該領域に該任意情報乃至該取り決めに基づくデータを該領域に保持することを特徴とする請求項１に記載の認証方式及び同方式による取引システム。

【請求項５】認証乃至取引は、原認証体と被認証体との間で暗号鍵を共有した状態で行われ、両体間の通信は該暗号鍵によって暗号化されることを特徴とする請求項１、２、３、４に記載の認証方式及び同方式による取引システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は認証システムに関し、更には、一連の商品取引過程に連動した認証システムに関する。

【０００２】

【従来の技術】パソコン通信ネットワークで、利用者（ユーザ）が当該ネットワークを利用し商品の購入や有料ソフトウェアのダウンロードをし、通信センタがその代金を自動引落し（信販会社経由含む）を行うシステムに於いて、代金の払い込みや商品の引き落し等の手続きをする上で、真の利用者を確認する手段、利用者の正当な取引を遂行する為の手段を備えた安全なシステムは存在しない。

【０００３】

【課題を解決するための手段】上記に鑑み本発明は、被認証体は秘密又は改ざん不可能な領域を有し、原認証体から送付された任意の情報乃至予め原認証体間で設定された取り決めを該領域に一時的又は一定の期間保持し、該任意の情報乃至該任意の情報に基づいたデータ乃至該

2

取り決めに基づいたデータよりなる戻りデータを原認証体に送付することにより、正当な利用者等の被認証体の認証ができ、利用者が安心して使用できるネットワーク、商品取引が形成され、簡便で安全な認証システムを実現した。又本発明によれば、ソフトウェアの販売を行うパソコン通信ネットワークに於いて、利用者が回線を使用して購入したいソフトウェアをダウンロードし、当該通信ネットワークセンタ（通信センタ）は、その利用者が予め通信センタに登録した銀行、又は信販会社経由で利用者が購入したソフトウェアの代金を引落すシステムの場合、利用者が他利用者になりすましてソフトウェアの購入が出来ないようにすることができるのである。更には、商品取引において、商品、サービスを提供する側（原認証体）がユーザ等の提供を受ける側（被認証体）へ、商品、サービスを提供する際、乱数などの任意情報をユーザに提供し、ユーザは秘密又は改ざん不可能な領域に保持し、ユーザが商品代金の支払等課金義務を履行する際、該戻りデータを商品、サービスを提供する側へ、送信し、戻りデータと任意情報とを比較検査し、一致乃至それに相当する場合だけ正当な取引であると認定することにより、不正な商品の重複提供がない唯一、一回の取引を実現することができるのである。本発明に於ける被認証体は、例えば、物品、ソフトウエアを購入し、その代金を支払う者又は、装置あるいは両者の組合せを示し、原認証体は、例えばこれら物品、ソフトウエアを販売する販売者あるいはその販売代金を請求する者それを代行する者あるいは、これらに相当する装置を示すがこれに限らず、互いに物品、ソフトウエアを売買することに関係する者あるいは装置あるいは両者の組合せであればよい。尚、本願発明では、その一例として商品乃至サービスを受ける利用者がＩＣカード、磁気カード等の少なくとも記憶手段を有する携帯型又は据置型の装置を所有しており、これらを含めて原認証体と示した。本発明で示す一時的又は所定期間とは、認証の必要が生じてから認証終了までの期間、あるいは商品取引が開始されてから対価の支払によって終了される迄、等が例示されるがこれに限られるものではない。又、原認証体が被認証体に送付する任意情報とは、原認証体が任意に作成するデータ、乱数データ、アルゴリズム等を示すが原認証体が任意に作成したものであればいかなるものであってもよい。被認証体が有する秘密又は改ざん不可能な領域とは、被認証体自信もその内容、その存在、あるいはその存在する場所を知らない領域あるいは知ったとしても改ざん不可能な領域を示すものであって、主にメモリー等で構成されるがその主旨に反するものでなければいかなるものであってもよい。改ざん不可能とは、内容を書き換えることが物理的に不可能であるという他、書換えは不可能ではないが、そこに留まる時間が不特定かあるいは極瞬間であり、実質不可能な場合等を示す。又、被認証体と原認証体が予め交わした取り決めとは、

例えば、その認証手続き時の日時等をしめす時系列的なデータであって、両者ともに必然的に同期するデータを戻しデータとして使用するという取り決めなどを示すものであるが特に限定されない。更に本発明では、認証を行う場合、互いに符号を共有した状態において起動されることが好ましい。この共有符号とは、例えば暗号鍵を示し、暗号鍵の共有システムを形成する場合特にＫＰＳ（Key Predisutribution system）方式がその手続きの簡便さ、ネットワーク会員の容易拡大性等からして好適である。又、原認証体と被認証体間の認証手続きのやり取りを行う場合においては、共有した符号をそのまま暗号鍵として用いて、暗号化によるやりとりができる点でも有効である。

ＫＰＳ方式

相手の識別子を自分固有の秘密アルゴリズムに施して相手と共有の鍵を作成する方式である。秘密アルゴリズムの作成、等の作業は主にセンタに於て行われ、独自にセンタアルゴリズムを所持し、このセンタアルゴリズムにユーザ等の被認証体、ソフトウェア及び商品、ソフトウェア供給体等の原認証体の識別子を施して、各々固有に所持される秘密アルゴリズムを作成する。センタアルゴリズムの作成方法、秘密アルゴリズムの作成方法、及び共有する暗号鍵の作成方法、エンティティ、識別子の定義等、共有鍵を作成するまでの行程に係わる方法及び内容は、特開昭６３年第３６６３４号公報、特開昭６３年第１０７６６７号公報に記載されている通りである。尚、識別子を秘密アルゴリズムに施す場合、上述の公報に記載されている方式の他、論文（松本、高嶋、今井　”簡易型一方向性アルゴリズムの構成”信学技報　ＩＴ８９－２３，Ｊｕｌｙ　１９８９）に記載された方式が好適に利用される。センタの作業はユーザ等の被認証体、商品、ソフトウェア供給体等の原認証体、これらの組合せが行ってもよい。尚、上述した鍵の使用方式は好適な一例であり、これらに限られるものではない。又、暗号アルゴリズムは、ＤＥＳ(DataEncyption Standard)、ＦＥＡＬ(Fast Data Encipherement Algorithm)（登録商標）等既存するものであれば構わないものである。

【０００４】

【実施例】以下本発明の実施例について詳述する。図１は、本発明が実施される際の環境例を示す。通信センタは、利用者のネットワーク加入申込みを受付けた後、利用者毎に異なる秘密アルゴリズムが入力され耐タンパー性のあるＫＰＳ暗／復号化器担体（Ｕｎ）を利用者に供給する、利用者はその担体Ｕｎをネットワークと接続されるパソコン等の情報端末に接続する、利用者がネットワークを使用し有料情報や商品の購入申込みをする際、通信センタは通信センタの秘密アルゴリズムが入力され耐タンパー性のあるＫＰＳ暗／復号化器担体（Ｃｎ）を使用し、その利用者の担体Ｕｎと通信センタの担体Ｃｎ

でのみ発生させられる共通鍵を使用し、次の詳細で述べる手段を用いて利用者の認証を行う。尚、ＫＰＳ暗／復号化器担体毎に異なる秘密アルゴリズムの生成と入力は通信センタ、又は秘密アルゴリズムを生成し入力する専用のセンタ、又はＫＰＳ暗／復号化器単体を製造する所のいずれでも可能で運用上好適の所で良い。又本技術は、課金のみならずパソコン通信サービスに於けるＣＵＧ（ClosedUser Group）でのアクセスコントロール、更には電子施錠式金庫の開閉等の、相手（使用者）認証が必要なものに応用が可能である。本発明において、認証が行われる前に行われる準備の一例を示す。

１、ユーザは通信センタに課金のための個人情報（Ｐｄａ）［例えば、パスワード、銀行名、口座番号、名前］を予め登録する。

２、通信センタは、通信センタ専用の秘密アルゴリズムＸｃが記憶された、ＫＰＳ暗／復号化器担体を準備する。

３、通信センタは、各ユーザにユーザ毎にユニークな秘密アルゴリズムＸｕが記憶されたＫＰＳ暗／復号化器担体を供給する。

【０００５】図２は、本発明の一実施例を示す図である。又図中の一点鎖線は外部から手を加えることが出来ない、耐タンパー性を有している部分である、更にＫＰＳ暗／復号器担体で使用される演算素子の制御は予め入力されたプログラムに従うもので外部から制御の変更が行えないものである。次に動作を説明する。

１、ユーザは、通信センタにユーザ識別子（ＫＰＳ－ＩＤｕ）を送出し、通信センタは、ユーザに通信センタ識別子（ＫＰＳ－ＩＤｃ）を送出する。

２、ユーザ及び通信センタは、それぞれの秘密アルゴリズムに相手の識別子（ＫＰＳ－ＩＤ）を作用させＫＰＳプロセスにより共通鍵（Ｋｃｕ）を作成する。

３、通信センタは、通信毎に変化する乱数ｒ０を発生させ共通鍵（Ｋｃｕ）で暗号化し（ｒ０’）ユーザへ送出する、又ユーザは共通鍵（Ｋｃｕ）でｒ０’を復号化しｒ０を求める。

４、通信センタは、ユーザに個人情報（Ｐｄｂ）［例えば、パスワード、銀行名、口座番号、名前］の入力要求［問題文］（Ｑｕ）を、先の乱数ｒ０で暗号化し（Ｑｕ’）ユーザへ送出する、又この時通信センタは送出した年月日、時刻（Ｔ０）をタイムスタンプとして一時記憶しておく。

５、ユーザは、通信センタからのＱｕ’を先の乱数ｒ０で復号化（Ｑｕ）し表示装置で確認後、個人情報入力要求に対する解答（Ｐｄｂ）［例えば、パスワード、銀行名、口座番号、名前］を入力し、又その時の年月日、時刻（Ｔ１）を自動又は手動で入力しＡｎｓとし、先の乱数ｒ０で暗号化し（Ａｎｓ’）、通信センタへ送出する。

６、通信センタは、ユーザからのＡｎｓ’を先の乱数ｒ

5

０で復号化し（Ａｎｓ）個人情報（Ｐｄｂ）、年月日、時刻（Ｔ１）とし、Ｐｄｂ及びＴ１が予め登録されたＰｄａ及び先のＴ０と一致しているかを検査し、一致している場合のみ正規のユーザとして認める、但しＴ０とＴ１の間に遅延時間が生じる恐れがあるため、Ｔ０又はＴ１にある程度の許容範囲を設けることが適当と思われる。ここで、Ｔ０及びＴ１はｒ０’、Ｑｕ’、Ａｎｓ’の再使用を防ぐのが目的であり、年月日、時刻又は通信センタとユーザとで同期して変化しているデータであれば何でも良い。

【０００６】更に、通信センタとユーザとで同期して変化しているデータが用意できない場合、図３に示す実施例による方式が好適と思われる、次に図３の動作説明をする。

１、ユーザは、通信センタにユーザ識別子（ＫＰＳ－ＩＤｕ）を送出し、通信センタは、ユーザに通信センタ識別子（ＫＰＳ－ＩＤｃ）を送出する。

２、ユーザ及び通信センタは、それぞれの秘密アルゴリズムに相手の識別子（ＫＰＳ－ＩＤ）を作用させＫＰＳプロセスにより共通鍵（Ｋｃｕ）を作成する。

３、通信センタは、通信毎に変化する乱数ｒ０を発生させ共通鍵（Ｋｃｕ）で暗号化し（ｒ０’）ユーザへ送出する、又ユーザは共通鍵（Ｋｃｕ）でｒ０’を復号化しｒ０を求める。

４、通信センタは、ユーザに個人情報（Ｐｄｂ）［例えば、パスワード、銀行名、口座番号、名前］の入力要求［問題文］（Ｑｕ）とその通信１回のみ通信センタで発生するデータ（Ｄｃｎ）を、先の乱数ｒ０で暗号化し（ＱＤ’）ユーザへ送出する。

５、ユーザは、通信センタからのＱＤ’を先の乱数ｒ０で復号化しＱｕとＤｃｎとしＤｃｎは一時記憶しＱｕを表示装置で確認後、個人情報入力要求に対する解答（Ｐｄｂ）［例えば、パスワード、銀行名、口座番号、名前］を入力し、先の一時記憶したＤｃｎを自動で入力しＡｎｓとし、先の乱数ｒ０で暗号化し（Ａｎｓ’）、通信センタへ送出する。

６、通信センタは、ユーザからのＡｎｓ’を先の乱数ｒ０で復号化し（Ａｎｓ）個人情報（Ｐｄｂ）及びＤｃｎとし、Ｐｄｂ及びＤｃｎが予め登録されたＰｄａ及び先のＤｃｎと一致しているかを検査し、一致している場合のみ正規のユーザとして認める。

【０００７】又、通信センタで利用者との通信１回毎に異なり、再使用されることのないデータが用意できない場合、図４に示す実施例でしめす方法が好適と思われる。次に図４の動作説明をする。

6

１、ユーザは、通信センタにユーザ識別子（ＫＰＳ－ＩＤｕ）を送出し、通信センタは、ユーザに通信センタ識別子（ＫＰＳ－ＩＤｃ）を送出する。

２、ユーザ及び通信センタは、それぞれの秘密アルゴリズムに相手の識別子（ＫＰＳ－ＩＤ）を作用させＫＰＳプロセスにより共通鍵（Ｋｃｕ）を作成する。

３、通信センタは、通信毎に変化する乱数ｒ０を発生させ共通鍵（Ｋｃｕ）で暗号化し（ｒ０’）ユーザへ送出する、又ユーザは共通鍵（Ｋｃｕ）でｒ０’を復号化しｒ０を求める。

４、通信センタは、ユーザに個人情報（Ｐｄｂ）入力要求［問題文］と通信毎に変化する乱数ｒを、先の乱数ｒ０で暗号化し（Ｑｕ’）ユーザへ送出する。

５、ユーザは、通信センタからのＱｕ’を先の乱数ｒ０で復号化し問題文と乱数ｒとしこれを一時記憶する。

６、ユーザは通信毎に変化する乱数ｒ１を発生させ共通鍵（Ｋｃｕ）で暗号化し（ｒ１’）通信センタへ送出する、通信センタは共通鍵（Ｋｃｕ）でｒ１’を復号化しｒ１を求める。

７、ユーザは、個人情報入力要求に対する解答（Ｐｄｂ）を入力し、又先の乱数ｒを自動的に入力し、先の乱数ｒ１で暗号化し（Ａｎｓ’）通信センタへ送出する。

８、通信センタは、ユーザからのＡｎｓ’を先の乱数ｒ１で復号化し個人情報（Ｐｄｂ）、乱数ｒとし、Ｐｄｂ及び乱数ｒが予め登録されたＰｄａ及び通信センタで一時記憶した乱数ｒと一致しているかを検査し、一致している場合のみ正規のユーザとして認める。ここで、個人情報Ｐｄａ、Ｐｄｂ及び通信センタでのそれらの一致検査を行わなければ、課金のみならず認証が必要な様々なシステムに使用できるものである。更に通信センタからの個人情報入力要求やユーザからの個人情報は、他の様々なデータに置き換えて使用しても良い。

【０００９】

【発明の効果】以上詳述のごとく本発明は、正当な利用者の認証ができ、利用者が安心して使用できるネットワークが形成され、簡便で安全な認証及びそれに基づく唯一の商品取引ができる等の効果を有する。

【図面の簡単な説明】

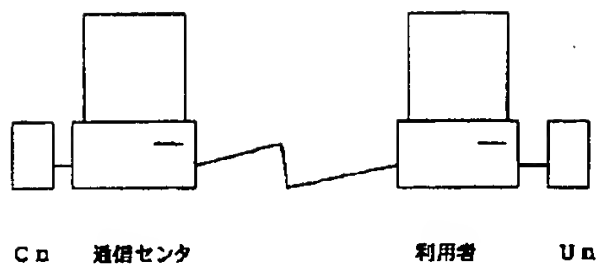
【図１】本発明を実施する為の環境の一例を示す図。

【図２】本発明の他の実施例を示す図。

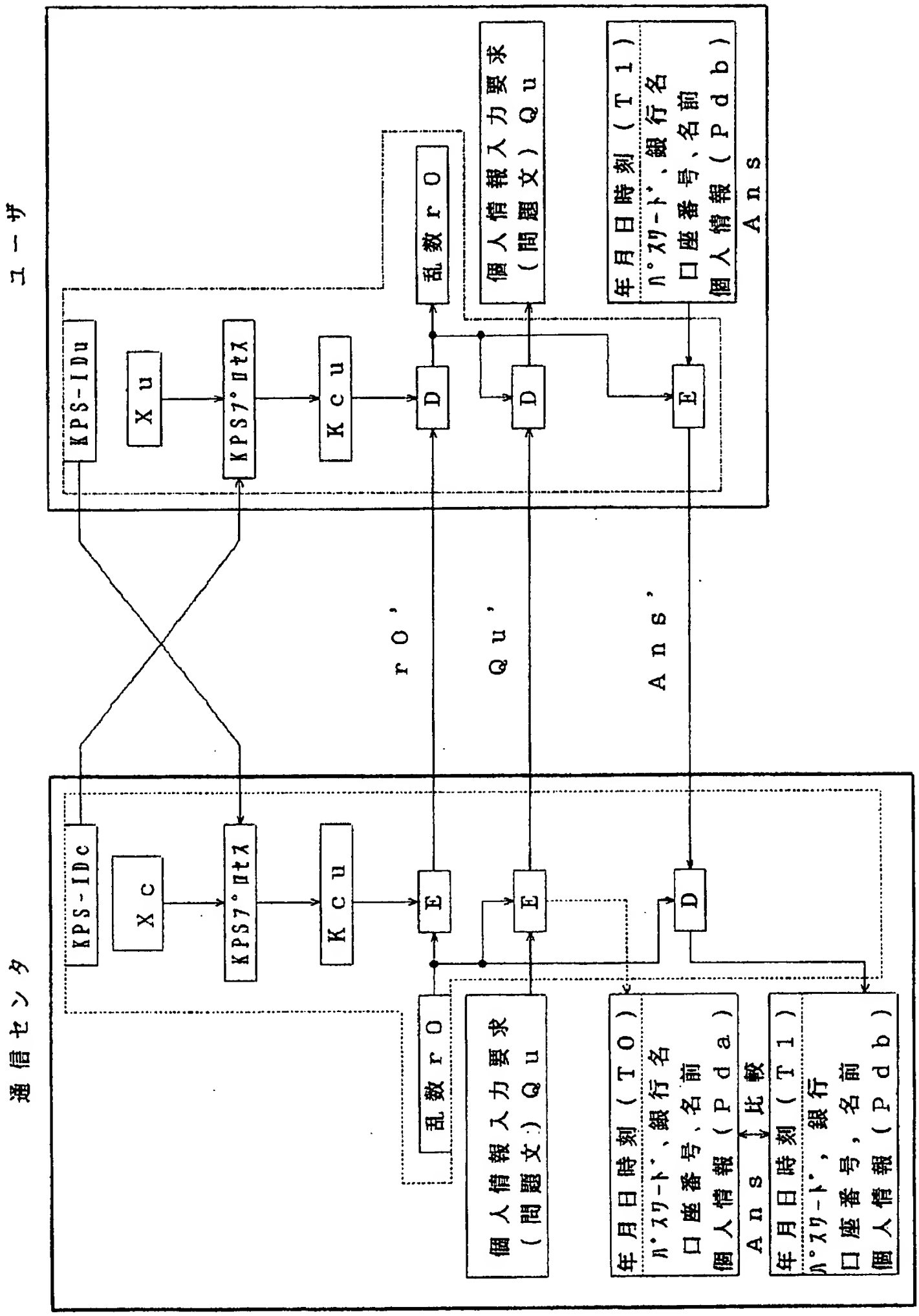
【図３】本発明の他の実施例を示す図。

【図４】本発明の他の実施例を示す図。

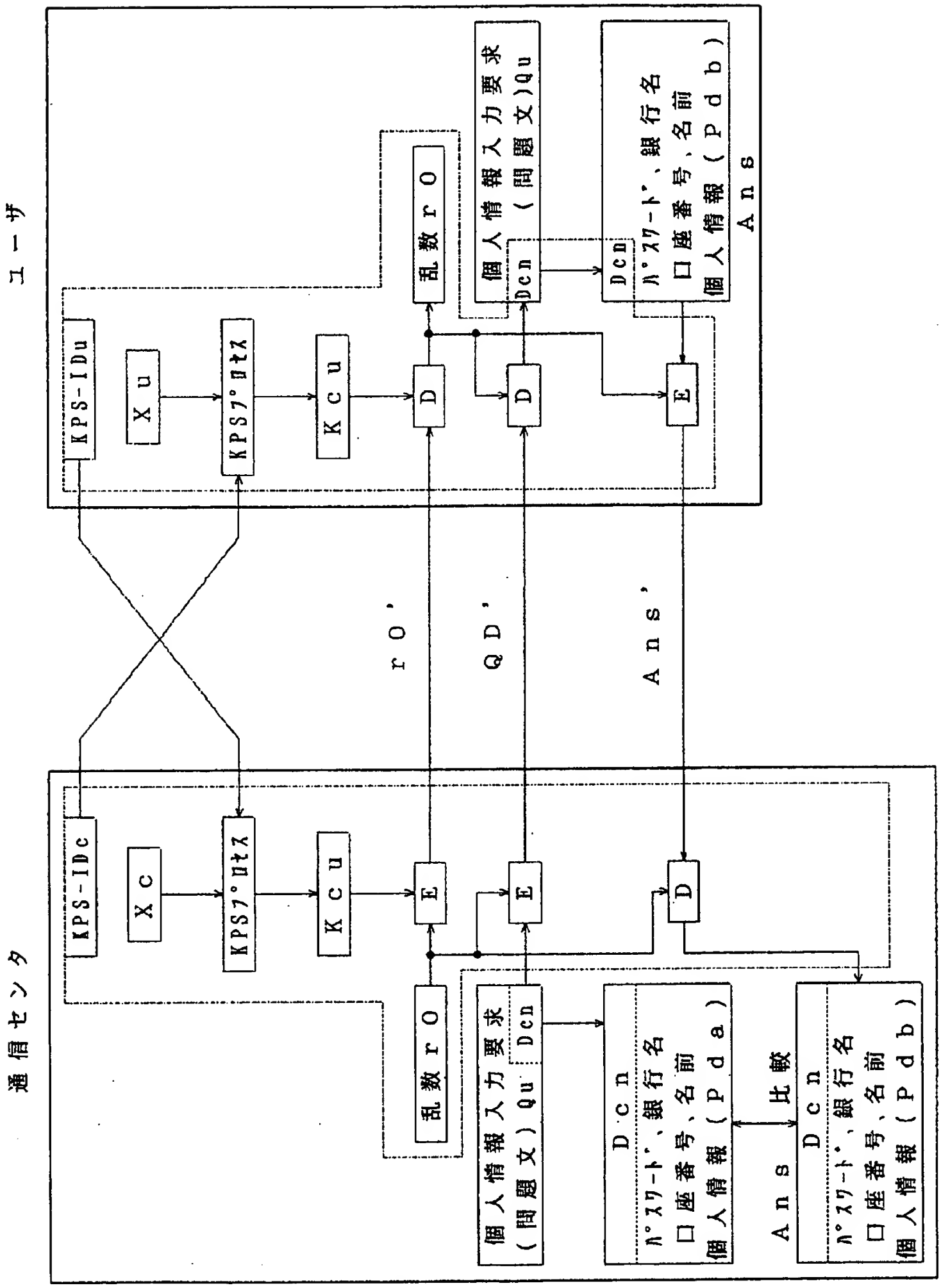
【図１】



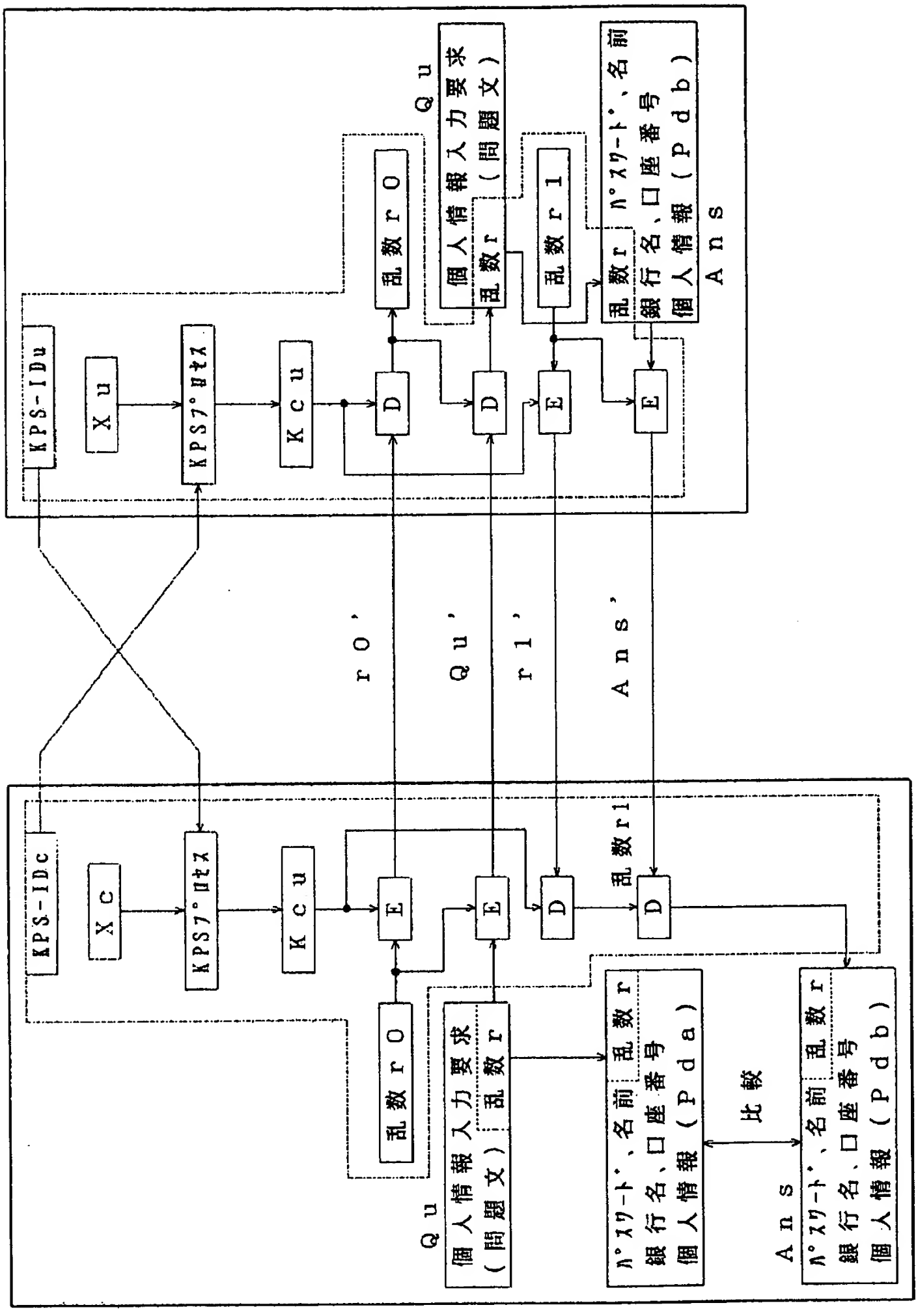
【図2】


ユーザ
KPS-IDu
Xu
KPSアロセス
Kcu
D
乱数rO
個人情報入力要求
（問題文）Qu
D
年月日時刻（T1）
ﾊﾟｽﾜｰﾄﾞ、銀行名
口座番号、名前
個人情報（Pdb）
Ans
E
rO'
Qu'
Ans'
通信センタ
KPS-IDc
Xc
KPSアロセス
Kcu
E
E
D
乱数rO
個人情報入力要求
（問題文）Qu
年月日時刻（TO）
ﾊﾟｽﾜｰﾄﾞ、銀行名
口座番号、名前
個人情報（Pda）
Ans ↔ 比較
年月日時刻（T1）
ﾊﾟｽﾜｰﾄﾞ、銀行
口座番号，名前
個人情報（Pdb）

【図3】


ユーザ
KPS-IDu
Xu
KPSアルゴ
Kcu
D
乱数r0
個人情報入力要求
Dcn
（問題文）Qu
Dcn
パスワード、銀行名
口座番号、名前
個人情報（Pdb）
Ans
D
E
r0'
QD'
Ans'
通信センタ
KPS-IDc
Xc
KPSアルゴ
Kcu
E
E
D
乱数r0
個人情報入力要求
（問題文）Qu'
Dcn
Dcn
パスワード、銀行名
口座番号、名前
個人情報（Pda）
Ans
比較
Dcn
パスワード、銀行名
口座番号、名前
個人情報（Pdb）

【図4】


KPS-IDu
Xu
KPSアルゴリズム
Kcu
D
乱数r0
D
個人情報入力要求
（問題文）
乱数r
E
乱数r1
E
乱数r　パスワード、名前
銀行名、口座番号
個人情報（Pdb）
Ans
Qu
r0'
Qu'
r1'
Ans'
KPS-IDc
Xc
KPSアルゴリズム
Kcu
E
E
D
乱数r1
D
乱数r0
個人情報入力要求
（問題文）
乱数r
パスワード、名前
銀行名、口座番号
個人情報（Pda）
比較
Ans
パスワード、名前
銀行名、口座番号
個人情報（Pdb）
乱数r
Qu

フロントページの続き

(51)Int.Cl.⁶	識別記号	庁内整理番号	FI	技術表示箇所
H04L 9/12				